Forum for Electromagnetic Research Methods and Application Technologies (FERMAT)

# Taking Lessons Learnt from EM into Other Domains

VIKRAM JANDHYALA

University of Washington

Vice Provost for Innovation @UW
UW Director, UW-PNNL Institute for Advanced Computing

SEPTEMBER 2014

# An Eclectic List

Web Search and Social Networks

Homomorphic Encryption

Machine Learning and Gaussian Processes

# Rank and Search on Graphs

PageRank – Simple and powerful early approach to ranking pages

PageRank equation :

$$P(i) = \alpha \sum_{j \to i} \frac{P(j)}{r_j^{out}} + \frac{(1-\alpha)}{n}$$

*S. Brin and L. Page, "The Anatomy of a Large-Scale Hypertextual Web Search Engine," Proc. 7th international conference on world wide web,1998.

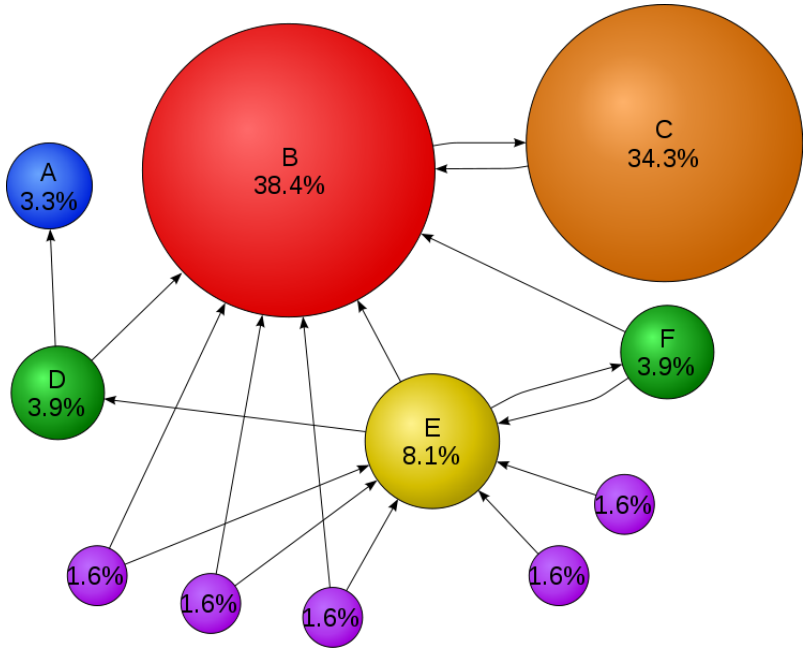



Image source : Wikipedia

# Observation: PageRank → Graph Helmholtz Formulation

Normalized PageRank of page *: $P_N(i) = \frac{P(i)}{r_i^{out}}$

$$P_N(i) = \frac{\alpha}{r_i^{out}} \sum_{j \to i} P_N(j) + \frac{(1-\alpha)}{n r_i^{out}}$$

After some algebra:

$$\frac{\alpha}{r_i^{out}} \left( P_N(i) r_i^{in} - \sum_{j \to i} P_N(j) \right) + P_N(i) \left( 1 - \frac{\alpha r_i^{in}}{r_i^{out}} \right) = \frac{(1-\alpha)}{n r_i^{out}}$$

Wavenumber : $k_i^{\,2} = \frac{r_i^{out}}{\alpha} - r_i^{in}$

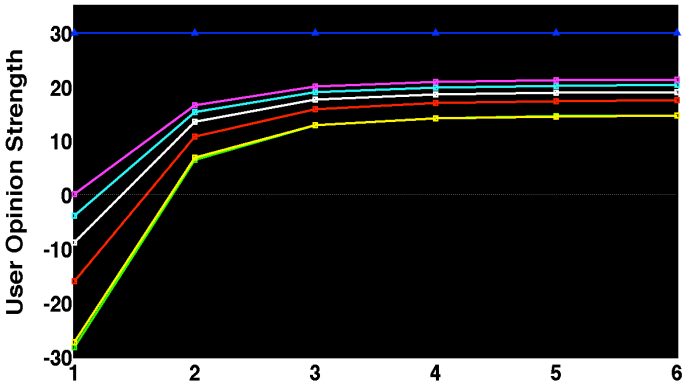
*V. Jandhyala, "Physics-Based Field-Theoretic Design Automation Tools for Social Networks and Web Search," Proc. 48th ACM Design Automation Conference, 2011.

# Special Case: The linear FJ Sociological model

The Friedkin-Johnsen (FJ) model [+] for opinion change

$$\boldsymbol{y}^{(t)} = \boldsymbol{AW}\boldsymbol{y}^{(t-1)} + (\boldsymbol{I} - \boldsymbol{A})\boldsymbol{y}^{(1)}$$

Closely connected group of *N* actors.




$y^{(t)}$ : actors' opinion at time 't'
$y^{(1)}$ : actors' initial opinions

***A*** : actors' susceptibility to interpersonal influence
***W*** : interpersonal influence weights

[+] N.E. Friedkin and E.C. Johnsen, "Social influence networks and opinion change," *Advances in Group Processes*, 16:1–29, 1999

# General Nonlinear interaction models+

Model 1

$$A_i(\omega) = F_i(\omega) + D_i^{\omega}\left(\sum_{j \to i} w_{ij}(\omega) A_j(\omega)\right)$$

Model 2

$$A_i(\omega) = F_i(\omega) + \sum_{j \to i} D_{ij}^{\omega}\left(w_{ij}(\omega) A_j(\omega)\right)$$

$i$ : $i^{th}$ user

$A$ : Total activity in terms of number of messages

$F$ : Intrinsic (or self) activity

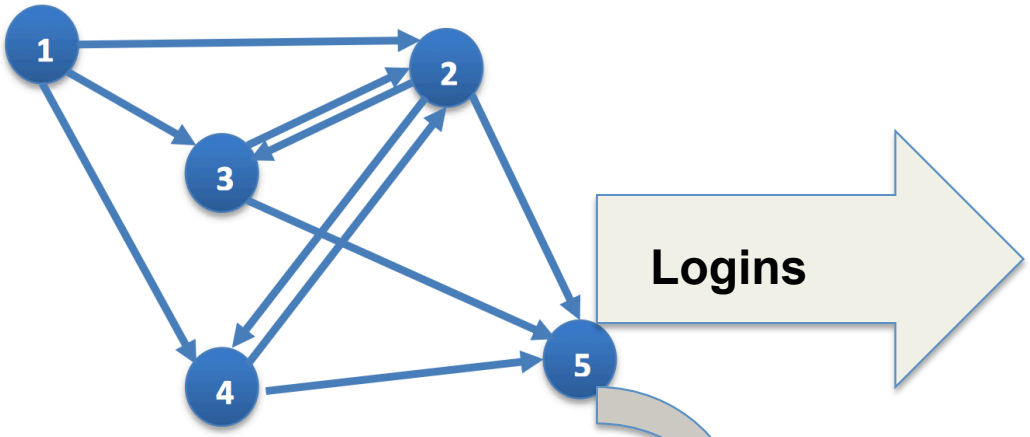
$D_i^{\omega}$ : Node specific operator operating on the feed

$D_{ij}^{\omega}$ : Edge (connection) specific operator operating on a part of the feed

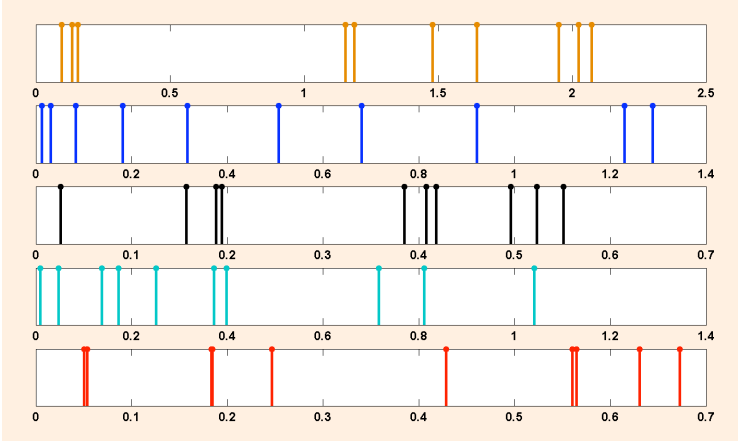
The above models are generalizations of the well known “Linear Threshold” model and the “Independent Cascade” model.

+ A.V. Sathanur, V.Jandhyala, C.Xing, “Design Automation for Large Scale Social Networks,” Design Automation Conference, San Jose, June 2013

# PhySense

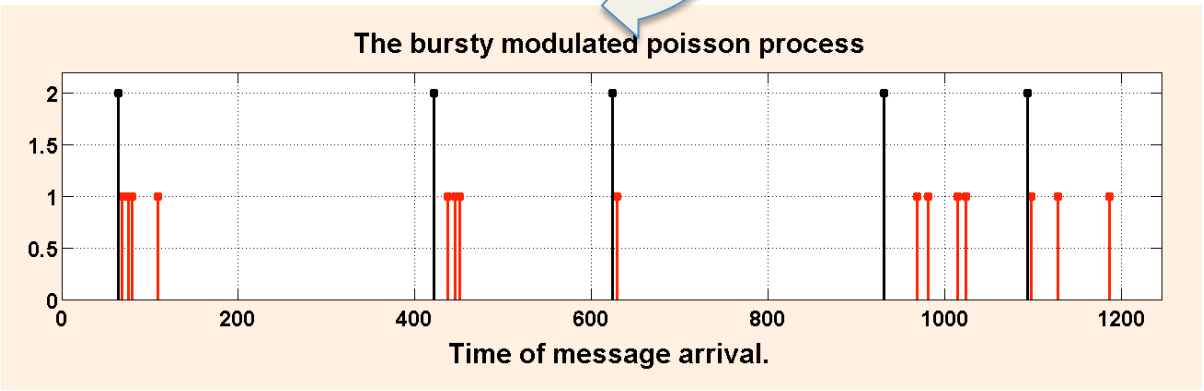



**Logins**




**Time axis in days**

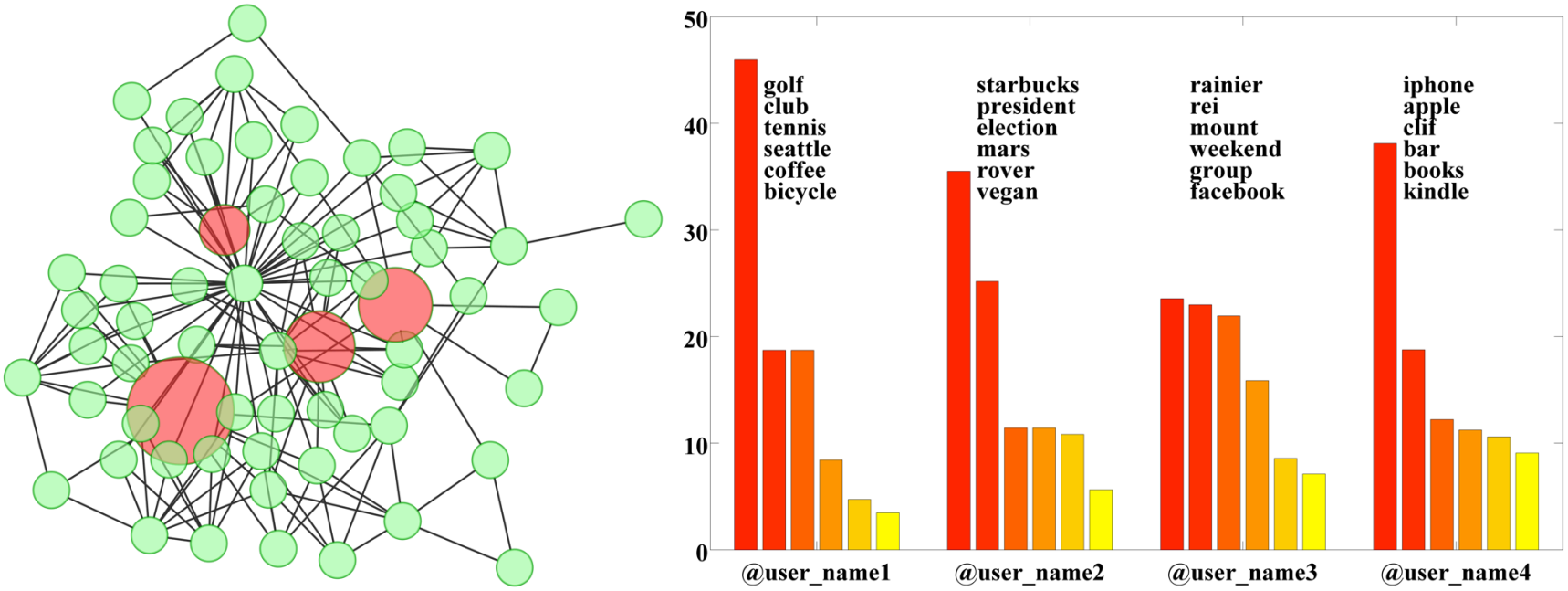
**Message timing**




**Time axis in minutes**

Each agent's activity is modeled by a modulated Poisson process with a slow logging-in rate and a high message firing rate. This is a special case of a Markov Modulated Poisson Process frequently used to model online human activity.

# Real Data: Influencer Analysis Through *PhySense*




Twitter influencers ( red nodes) and their other interests ranked by their activity composition over a time window. Influencers are identified by measuring their *activity propagation potential* and *not* just by follower count or number of tweets.

# Cloud Security

Reality and Perception of Critical IP on a Public Cloud:

Many organizations to whom scalable computing is critical will NOT use the Public Clouds on sensitive data or IP even though it would provide a huge cost saving and productivity multiplier

Why ?

IP/Data is decrypted on the cloud prior to computation

IP/Data is as secure as the key; Prone to key-compromise.

*SimX*

# An Engineering Approach to Scalable Homomorphic Encryption

# Homomorphic encryption - intro

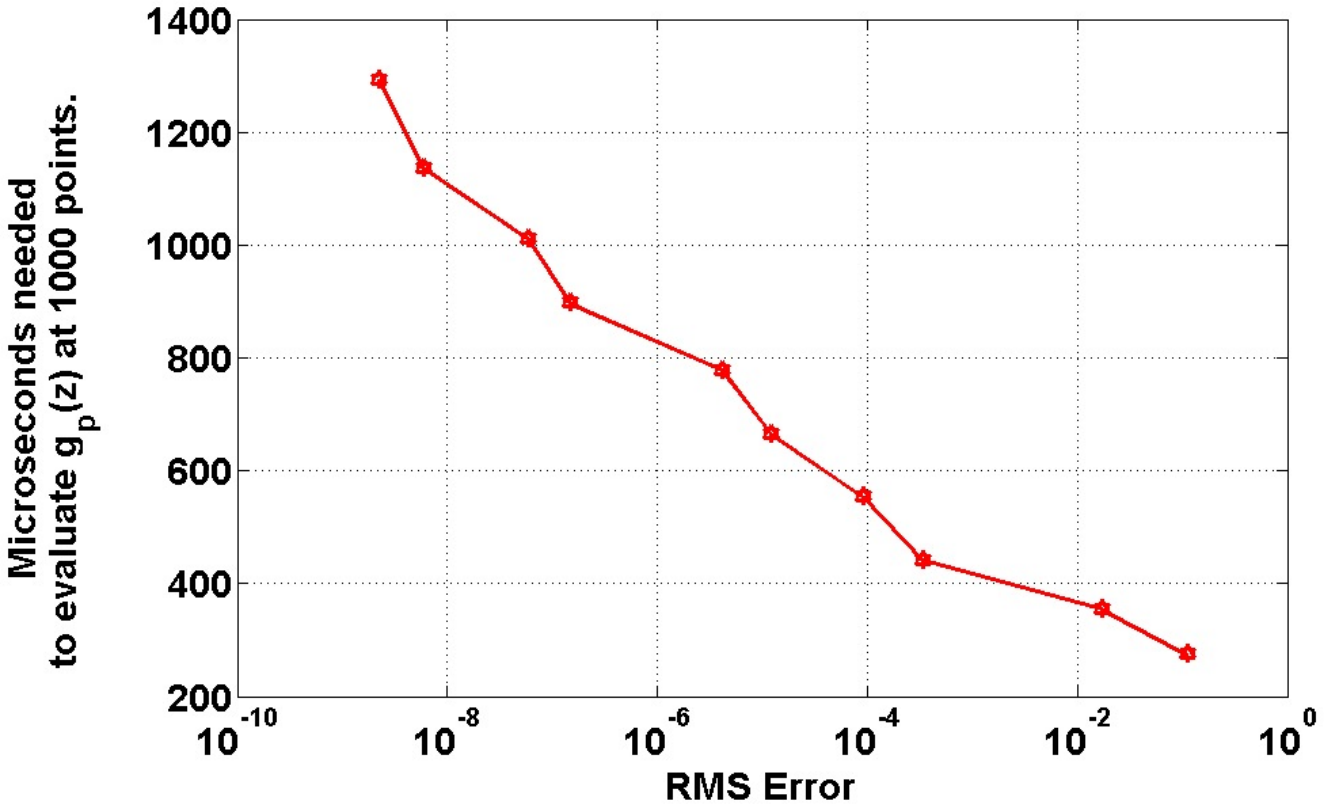
- Homomorphic Encryption allows arbitrary computations in the encrypted domain

- Support for basic binary operations at the circuit level translates to support for arbitrary computation

$$E(x_1)+E(x_2) = E(x_1)+E(x_2)$$

$$E(x_1).E(x_2) = E(x_1,x_2)$$

# Trading off complexity and accuracy in the function composition approach



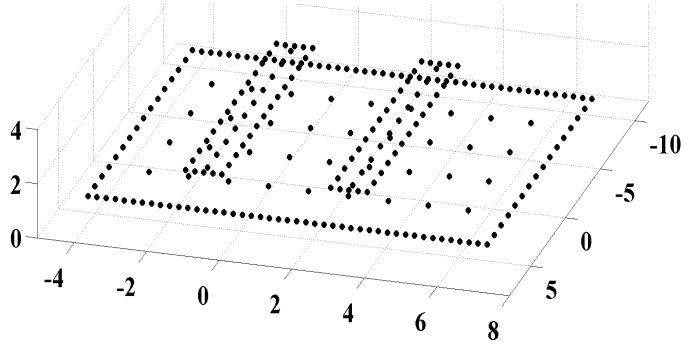

*f(x)*= desired computation

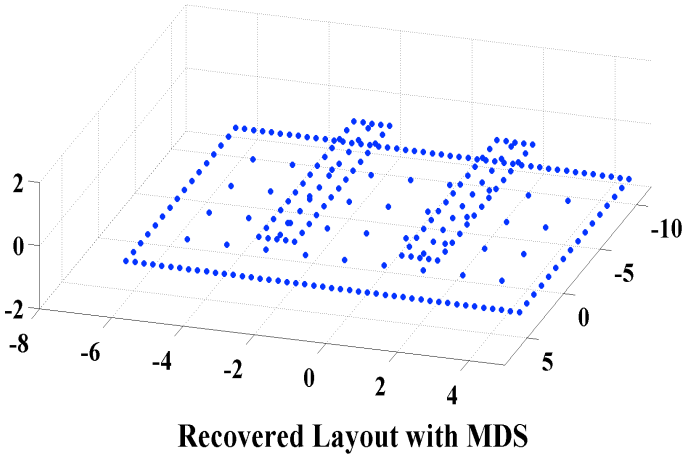
*z=h(x)* = encrypting function

$$h_p(x) = px$$

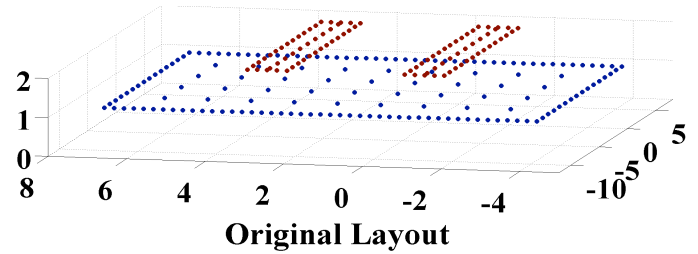
$$f(x) = log_e\left(1 + \frac{x^4}{2}\right)$$

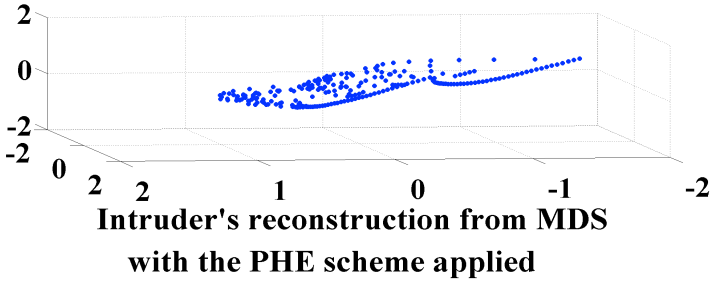
# IP reconstruction

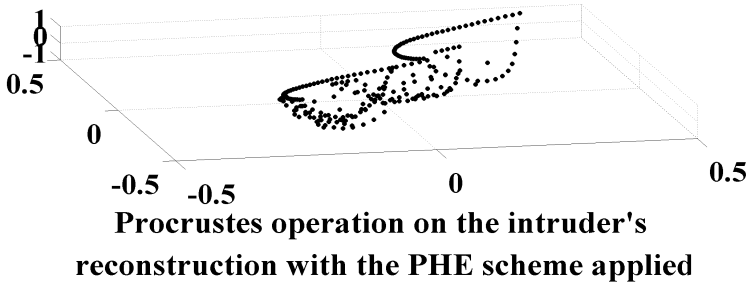



Hacker can reconstruct IP from Green's function matrix without encryption

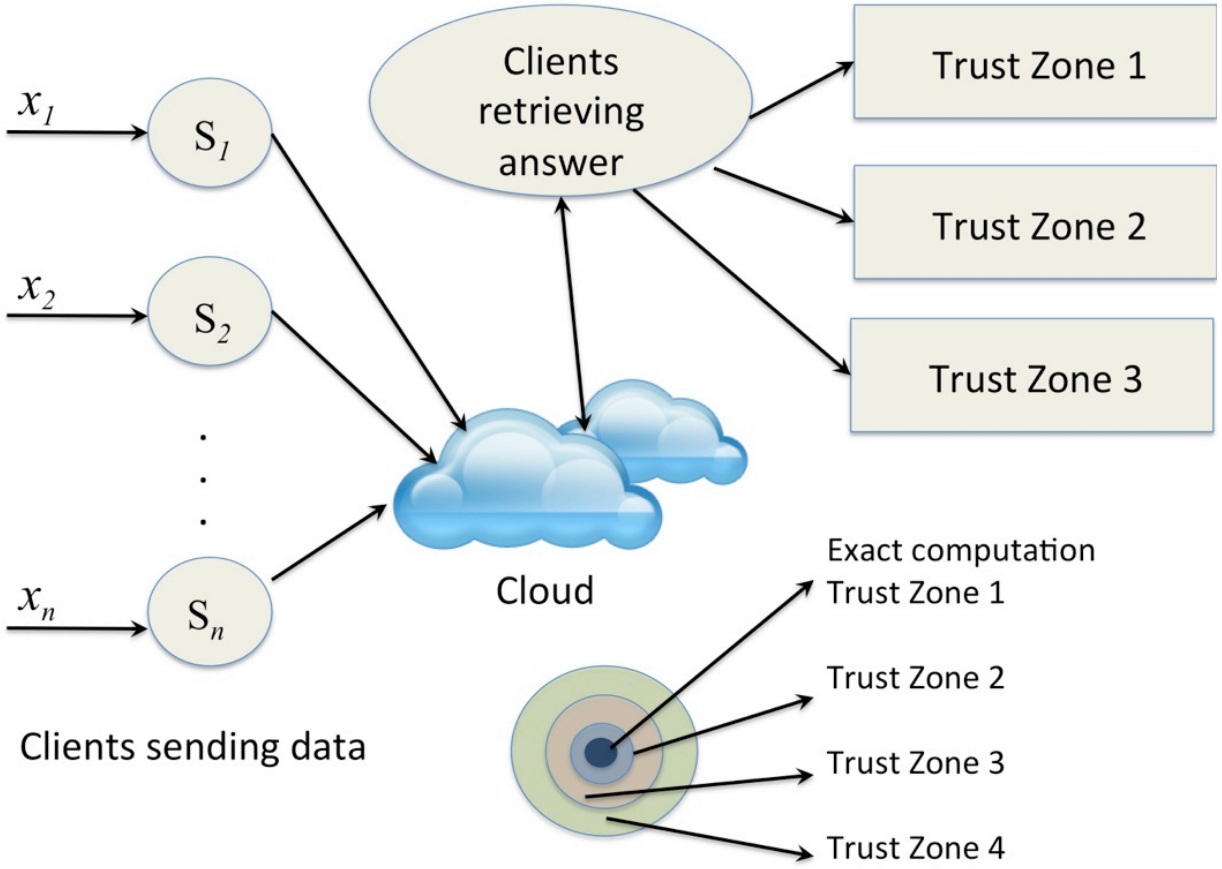



Hacker cannot reconstruct the IP from Green's function matrix with the PHE scheme applied

# An interesting side-effect - Multi-scale encryption



# Leadership Lessons

## Resolving Disputes

Getting the Job Done

# Chips > > # Aeroplanes

# The REAL Talk

A socially awkward, easily impressionable, protected and spoiled, Indian kid goes to study and work at the world's premier EM group

# You “Want” To Take this Course

No I don’t.

# Prof. Mittra, are you Taking this Course ?

Offering. Offering.

# Do You Have a Rubber ?

Its called an Eraser.

# Condo Open House

Not a place to collect free contraceptives

# White Noise

-- A loud, opinionated expert of Caucasian descent

# The  Red Jag Convertible

-- Saturday morning: IMPE or EM ?

# The Most Amazing Place

Dedicated, brilliant faculty members
A huge pool of brilliant students and researchers

EMC Lab, CCEM, ECE@UIUC

# My First Job

A simple static FMM

Wonderful GUIs

A QA guy to test my code for me

Great pay!

# Thank You

Our kids ←My wife ← Met at a VC firm while I was raising money for Physware (Nimbic) (Mentor) ← DARPA funded EM project <- EM ← UIUC and Raj!

# Thank You

Thank You Raj

Thank You EM @ UIUC

Thank you ECE@UIUC